SanDisk

Cruzer Enterprise

Product Specifications

Revision 1.0

Document No. PSP-CRE-0507-11

May, 2007

SanDisk Corporation

Corporate Headquarters • 601 McCarthy Blvd. • Milpitas, CA 95035

Phone (408) 801-1000 • Fax (408) 801-8657

www.sandisk.com

Table of Contents

1. Scope

This Product Specification document provides product and technical information for the Cruzer Enterprise using the S2 controller. This document is intended for System and IT Administrators who are responsible for the care and maintenance of the Cruzer Enterprise.

2. Product Overview

Cruzer Enterprise offers the following features:

- Cruzer Enterprise is 2.0 High Speed compliant and 1.1 Full Speed compatible
- The drive is fully secured using a sophisticated password mechanism
- Cruzer Enterprise includes a 256-bit AES hardware-based encryption

Cruzer Enterprise can be managed using Cruzer Enterprise CMC, a software based interface that provides corporate networks with security against internal threats and loss of corporate sensitive data, while securing data residing on corporate issued Cruzer Enterprise drives.

As with any USB Flash drive, the Cruzer Enterprise drive can be used to store data. However, all information on the Cruzer Enterprise is securely stored and encrypted with a 256-bit AES hardware based encryption. It is also secured using a sophisticated password protection method. In addition, the Cruzer Enterprise includes a “lockdown” mode for enhanced security. This lockdown feature will lock the Cruzer Enterprise whenever a maximum number of password attempts exceed a pre-configured value. In the event that the device is locked, the device must be reformatted to enable operation. All data on the Cruzer Enterprise will be erased.

2.1 Product Architecture

The Cruzer Enterprise is based on the SanDisk S2 controller, which is designed for data storage applications. It combines these storage capabilities with a self-contained system based on the ARM7-TDMI 32-bit RISC processor to enable a wide range of applications. Users can extend device functionality with applications based on the S2 platform to secure files, personalize the user interface, and other functions.

The following diagram illustrates the main functional blocks of the S2 controller:

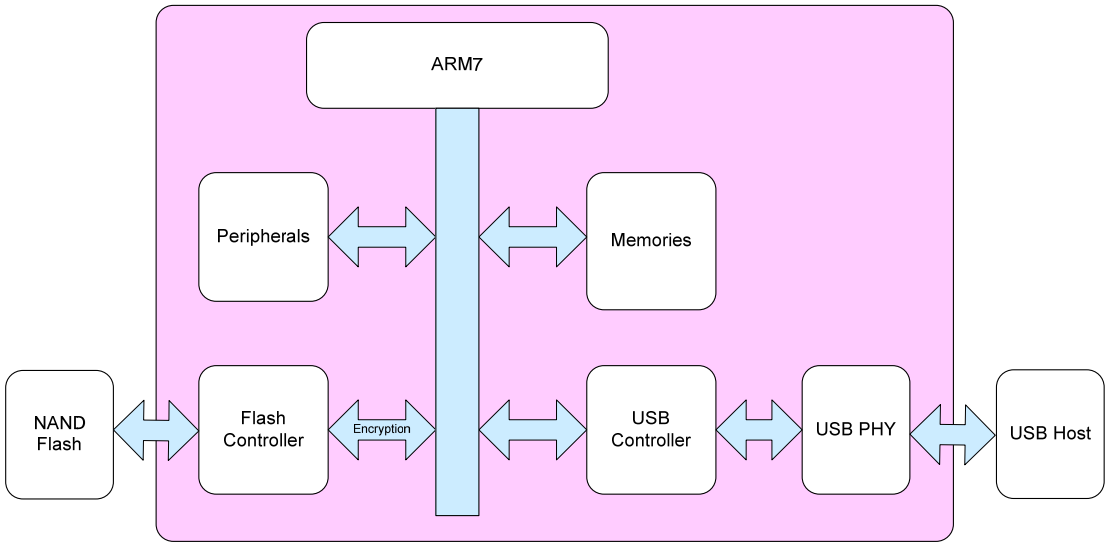

Figure 1: S2 Controller Architecture

2.2 Data Security

The Cruzer Enterprise security architecture combines hardware-based access control and security features that are insulated from the host computer environment.

Cruzer Enterprise implements a double security mechanism, access control and data encryption, based on SHA-1 and AES algorithms. Encrypted data is stored in a secure zone, hidden until successful authentication is completed by the Cruzer Enterprise access control mechanism. This method of encryption and authentication is more secure than software commands. Data is encrypted and decrypted dynamically within the device, thus only data required by the host PC is decrypted and sent to the PC.

2.2.1 Access Control - Maximum Number of Attempts (Max NOA)

Cruzer Enterprise locks automatically for further access after a predefined number of consecutive, incorrect password attempts. This number is defined during the manufacturing process. This feature prevents *brute force attacks*, where the hacker tries several password variations in order to determine the correct password.

2.2.2 Encryption Algorithms

Cruzer Enterprise implements industry-standard symmetric and asymmetric algorithms. No proprietary algorithms are used.

Symmetric Algorithm

Cruzer Enterprise supports the symmetric AES algorithm described in Table 1.

The Parallel AES Coprocessor is used for fast computation of the Advanced Encryption Standard algorithm. The AES algorithm is described by the FIPS PUB 197 Advanced Encryption Standard.

Table 1: Symmetric Algorithm used by Cruzer Enterprise

Encryption Algorithm	Key Length	Encryption Mode
AES	256-bit	TDEA Electronic Code Book (TECB)

Figure 2 illustrates the encryption flow using the Electronic Code Book (ECB) encryption mode. Details of the encryption and decryption cycles follow.

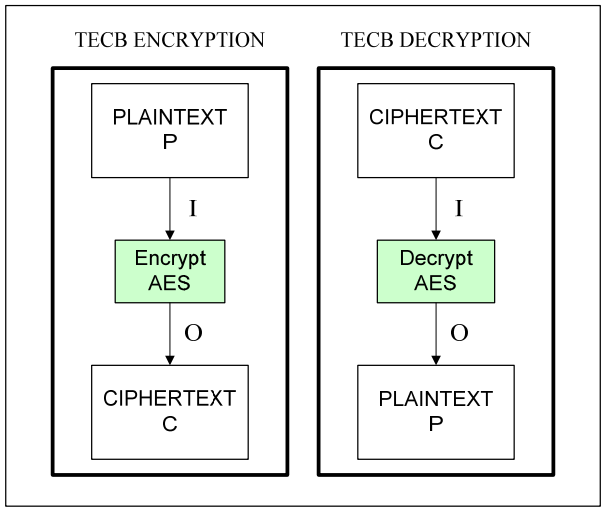

Figure 2: TDEA Electronic Code Book (TECB) Mode

In TECB encryption, a 256-bit plaintext data block (P) is used directly as the input block (I). The input block is processed through the AES encoder using a 256-bit key. The resulting 256-bit output block (O) is used directly as ciphertext (C).

In TECB decryption, a 256-bit ciphertext block (C) is used directly as the input block (I). The input block is processed through the AES decoder using the same 256-bit key. The resulting 256-bit output block (O) produces the plaintext (P).

Hashing Algorithm

Cruzer Enterprise implements a SHA-1 hash function as part of access control and creation of a symmetric encryption key for flash data.

Random Number Generator

Cruzer Enterprise implements a hardware Random Number Generator.

2.3 System Requirements

The system requirements for the Cruzer Enterprise are as follows:

- Pentium III processor
- 10 MB free disk space
- USB 1.1 port* (For best performance, it is recommended to use a USB 2.0 port)
- Operating Systems:
  - Microsoft Windows 2000 SP4 and higher
  - Microsoft Windows XP SP1 and higher
  - Microsoft Windows XP 64-bit SP1
  - Microsoft Server 2000
  - Microsoft Server 2003 (Standard and Enterprise Editions)
  - Microsoft Vista (all editions)

Note: For Windows 2000 users without administrative privileges, USB 2.0 port is required.

2.4 Product Warranty

The Cruzer Enterprise has a warranty period of two (2) years.

3. Product Specifications

3.1 Flash Type

The Cruzer Enterprise contains Single-Level Cell (SLC) NAND flash.

3.2 Interface

The Cruzer Enterprise employs the following interfaces:

- USB 2.0 high-speed
- USB 1.1 compliant (not recommended because of slow transfer rates)

3.3 Capacity

3.3.1 Flash

Table 2: Flash Capacity

Device Capacity (GB)	Number of Flash Chips
1	2
2	2
4	2;4
8	4

3.3.2 Drive / User Area

Table 3: Cruzer Enterprise User Area Capacity (FAT File System)

	1 GB	2 GB	4 GB	8 GB
User Area Capacity (KB)	950,528	1,970,400	3,843,212	8,192,820

3.4 Supported Operating Systems

See System Requirements for a list of supported operating systems.

3.5 Device Configuration

The device consists of the following configuration:

- 1 read-only partition (appears as CD-ROM drive to the operating system)
- 1 secure removable partition (appears as a removable USB flash drive to the operating system)
- 1 hidden partition (not accessible to the operating system)
- Customer-specified content can be placed on the device during manufacturing

3.6 Performance

Performance was measured using industry-standard benchmark software.

USB 2.0 High Speed

480 Mbit/sec high-speed USB compatible

Table 4: Cruzer Enterprise Transfer Speed (Minimum)

Capacity	Multiple Flash (MB/s)
1 GB	24/20
2 GB	24/20
4 GB	24/20
8 GB	24/20

3.7 LED Functionality

LED Functions:

- **No LED is visible** - Cruzer Enterprise is connected and inactive
- **LED is flashing** - Cruzer Enterprise is transmitting or receiving data or is in the identification process

3.8 Certifications and Standard Compliance

Cruzer Enterprise has the following certifications:

- USB high-speed certification (high power device)
- FIPS 197 AES engine (CAVP certificate #464)
- WHQL for Windows 2000, Windows XP, and Windows Vista
- FCC
- CE

4. Electrical Specifications

4.1 Power Mode

The Cruzer Enterprise is identified as a high-powered device.

4.2 DC Characteristics

Table 5: DC Characteristics for Full-Speed and High-Speed Operation (TA = 25°C,VDD = 3.3v, VSS = 0V)

Parameter	Symbol	Test Conditions	Min	Typ	Max	Unit
USB Signals						
Supply Voltage:	VBUS		4.40	5.00	5.25	V
Supply Current (RMS)	Icc	VBUS=5.0v	--	<100	<180	mA
Operating:	Iccs		--	<500	<500	µA
Suspend:						

5. Environmental Specifications

5.1 Temperature

Operating temperature: 0° C to 60° C

Storage temperature: -40° C to 70° C

5.2 Humidity

Relative humidity during operation (non-condensing): 5% to 90%

Relative humidity during storage: 5% to 95%

5.3 Altitude

Operating: Low Altitude Limit: -200 m; High Altitude Limit: 6,096 m (20,000 ft)

Non-operating: Low Altitude Limit: -200 m; High Altitude Limit: 12,192 m (40,000 ft)

5.4 Vibration (Random)

Operating: 5 G RMS, 10 to 2,000 Hz, 0.5 Oct/min sweep rate

Non-operating: 10 G RMS, 10 to 2,000 Hz, 0.5 Oct/min sweep rate

5.5 Shock

Operational Half-Sine Shock: The device withstands operational half-sine shock of 90 in/sec (179 g peak) 2 shocks in 3 directions duration 2ms.

Non-Operational Half-Sine Shock: The device withstands operational half-sine shock of 90 in/sec (179 g peak) 2 shocks in 3 directions duration 2ms.

5.6 Crush

The device withstands 3.3kgf/cm^2 of sustained force on all three axes without any damage.

5.7 Drop Test

The device withstands 2 drops on concrete floor from 60 inches on each of 6 axes without any damage.

5.8 Dust Protection

The internal protection corresponds to level IP50 according to IEC 60529.

5.9 Restricted Materials Content and RoHS Compliance

Cruzer Enterprise complies with the Restriction of Hazardous Substances (RoHS) directive, as well as the directive regarding lead-free products.

In addition, Cruzer Enterprise does not contain any material that is listed as restricted in the 2002/95/EC directive issued by the European Parliament.

SanDisk® Corporation general policy does not recommend the use of its products in life support applications where in a failure or malfunction of the product may directly threaten life or injury. Per SanDisk Terms and Conditions of Sale, the user of SanDisk products in life support applications assumes all risk of such use and indemnifies SanDisk against all damages. See "Disclaimer of Liability."

This document is for information use only and is subject to change without prior notice. SanDisk Corporation assumes no responsibility for any errors that may appear in this document, nor for incidental or consequential damages resulting from the furnishing, performance or use of this material. No part of this document may be reproduced, transmitted, transcribed, stored in a retrievable manner or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written consent of an officer of SanDisk Corporation.

All parts of the SanDisk documentation are protected by copyright law and all rights are reserved.

SanDisk and the SanDisk logo are registered trademarks of SanDisk Corporation. CompactFlash is a U.S. registered trademark of SanDisk Corporation.

Product names mentioned herein are for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

SanDisk products are covered or licensed under one or more of the following U.S. Patent Nos. 5,070,032; 5,095,344; 5,168,465; 5,172,338; 5,198,380; 5,200,959; 5,268,318; 5,268,870; 5,272,669; 5,418,752; 5,602,987. Other U.S. and foreign patents awarded and pending.

Lit. No. Revision 1.0 Rev. 1.0 05/07 Printed in U.S.A.

Revision History
May 2007 Revision 1.0—initial release